Siber Terörizm Nedir?

Siber Terörizm Nedir?[i]

Teknolojinin gelişmesiyle birlikte terörizm kendisine yeni alanlar ve yeni yöntemler bulmuştur. Terör örgütleri bir yandan kırsalda ve şehirlerde terör faaliyetlerini devam ettirirken diğer yandan kendilerineyeni bir alan yaratmış, siber alanda da faaliyet göstermeye başlamışlardır.

Bu çerçevede siber terörizm, belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı, bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır. Siber terörizmde, ulusal bankacılık sistemlerinin çökertilmesi, insanlara ait hesapların ele geçirilmesi, devlete ait gizli bilgilerin bu yolla elde edilmesi, resmi ve sivil internet sitelerinin çökertilmesi gibi birçok faaliyet icra edilebilmektedir (Şimşek, 2016, s.325).

Siber terörizm kavramının, ortak kabul edilmiş bir tanımı bulunmadığından, ucu açık bir kavram olarak kabul edilmektedir. Terörizm tanımı ve bu saldırıların sayısal ortamlarda gerçekleştirildiği göz önünde bulundurulduğunda siber terörizm; bireylerin veya toplumların can ve mal güvenliğini riske atmak/zarar vermek için etkileşimde bulundukları, sayısal teknolojilere ve/veya platformlara gerçekleştirilen saldırılar olarak tanımlanabilir (Atasever vd., 2019, s.239).

Başka bir bakış açısına göre siber terörizm, psikolojik, sosyal, siyasi ve dini güdülere sahip ya da bu güdüler ile hareket eden, bilgisayar ağı ve teknolojisi kullanarak ulusal savunma sistemlerine, hükümete ait varlıklara saldırarak, bireylere ya da değişik gruplara yönelik olarak zarar verici faaliyet içinde bulunan bir terörizm şeklidir (Şimşek, 2016, s.325).

Siber terörizm kapsamındaki saldırılar genel olarak beş farklı kategori altında incelemektedir.

1- Saldırı: Siber teröristin temel amacı bir ağa erişerek bilgi elde etmek ya da sistem içerisindeki bilgileri değiştirerek diğer tarafa karşı avantaj elde etmek istemektir. (Gizli hükümet bilgilerini ve kişisel bilgileri çalmak gibi).

2- Tahribat: İsminden de anlaşılacağı üzere asıl amaç bilgisayar sistemlerini yok etme veya zarar vermektir. 2007 Estonya saldırıları verilebilecek en önemli örneklerden bir tanesidir.

3- Dezenformasyon: Bu tip saldırıların amacı söylentiler aracılığıyla hedef devlet içerisinde korku ve kaos ortamı yaratmaktır.

4- Hizmet Dışı Bırakma: Bu tip saldırıların amacı çevrimiçi bilgisayar sistemlerini kilitlemektir.

5- Web Sitelerini Tahrif Etme: Bu tip saldırılarda ise amaç web sitelerini bozmak ya da tahrif etmektir. Temel amaç web sitesi içerisindeki bilgileri tahrif ederek terör örgütlerinin propagandasını yapmak için elverişli hale getirmektir (Erendor, 2016, s.123-124).

Özcan'a göre siber terörizm, belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır (Özcan, 2002, s.309). Bu tanımda siber terörizmin aracı olarak bilgisayar sistemleri, hedef olarak ise hâkim otoritenin ve toplumun baskı altında tutulmasının söz konusu olduğu ifade edilmektedir.

Siber terörizm, siyasi ve sosyal mercilere, kişi ve kurumlara gözdağı vermek, baskı oluşturmak amacıyla resmi kuruluşların bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Üzerinde durulması gereken önemli noktalardan biri de bir saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi ve/veya en azından korku yaratacak kadar hasara yol açması gerekmektedir. Ülkelerin kritik alt yapı sistemlerine yapılan saldırılar da, yarattığı etkiye göre, siber terörizm olarak tanımlanabilir (Yılmaz, 2020, s.70).

Siber terörizm, devletlerin bilişim sistemlerine yasa dışı yollarla ele geçirmesi veya nüfuz etmesi sonucunda devlet kurumlarının alt yapılarına zarar vererek, toplum düzenini bozacak ekonomik ve sosyal alanda toplumun huzuru bozacak eylemler olarak tanımlanabilir. Siber eylemlerin söz konusu etkileri dikkate alındığında, karşımıza yeni bir terörizm çeşidi çıkmaktadır (Hatipoğlu, 2017, s.165).

Siber terörizmin amacı, bilgisayar ağlarını kullanılamaz hale getirmeye yönelik istemli olarak yapılan, geniş kapsamlı eylemleri de içerisinde barındırmak üzere, terör eylemlerinde internete bağlı kişisel bilgisayarları kullanmak ve internet tabanlı saldırılar yapmaktadır. Siber saldırı yönteminin terör grupları tarafından kullanılmasının en önemli nedenlerinden biri saldırıyı düzenleyen kişilerin takip edilmesinin oldukça zor olmasıdır. Siber saldırı yöntemi, gerçek dünyada meydana gelen saldırı yöntemlerine göre daha anonim bir kimlikle yapıldığı için saldırıyı düzenlemekte olan gruplar bir gümrük noktası veya havaalanı kontrolünden geçmeden hedef ülkeye ulaşabilmektedirler (Yılmaz, 2020, s.70)

Siber terörizm, bilgisayar ağlarını kullanarak kritik öneme sahip ulusal altyapılara (enerji, ulaşım ve devlet işlemleri) zarar vermeyi ya da tamamen kullanılamaz hale getirmeyi amaçlayan saldırılar biçiminde kendini göstermektedir. Siyasal bir amaç uğruna insanlara zarar vermek veya acı çektirmek için devlet tarafından iyi korunan alanlardaki (telekomünikasyon, ulusal güvenlik ağları vs) bilgileri elde etmek, değiştirmek veya terörist amaçlar için kullanmak siber terörün önemli hedefleri arasında yer almaktadır (Gürkaynak ve İren, 2011, s.268).

Siber terörizmin sadece fiziksel saldırı değil aynı zamanda psikolojik saldırı amacıyla kullanıldığı da iddia edilmektedir. Bu çerçevede ele alındığında siber terörizmin propaganda saldırılarıyla ilgili olarak çarpıcı örnek olaylara değinmekte de fayda görülmektedir. Bunlardan belki de ilki 1996 yılında Peru'nun Lima şehrinde Japon Büyükelçiliğine saldırarak diplomatik, askeri ve siyasi

personeli rehin alan Tubac Amaru adlı terör örgütünün ABD'de ve Kanada da bulunan sempatizanları örgütün faaliyetini destekleyen birçok site kurmuşlardır. Bu sitelerde, propaganda ve eyleme destek ile birlikte örgütün Japon Büyükelçilik binasına saldırı planlarını da yayınlamışlardır.

İslam dinini meşruiyet kaynağı olarak kullanan terör grupları, interneti ayrıca Batı karşıtlığı ve anti İsrail propagandaları için kullanmakta ve yaymaktadırlar. Hamas taraftarlarınca oluşturulan bazı internet siteleri örgütün patentini, siyasi ve askeri bildirilerini taşımaktadır ki bu bildirilerin bir kısmı Yahudilerin öldürülmesini istemektedir. İngiltere'de faaliyet gösteren Hizbut Tahrir örgütü ise İngiltere'de düzenli yapılan toplantıları hakkında web sitesi aracılığıyla, halka ayrıntılar sunmaktadır. İran destekli Şii terörist örgütü Hizbullah ise Güney Lübnan'da web siteleri aracılığıyla kitaplar satmaktadır. Bazı İsrail ve ABD resmi kaynakları, teröristlerin patlayıcıların nasıl kullanılacağı hakkında, yoldaşlarını harita, fotoğraf, talimat, kod ve teknik detaylar aracılığıyla eğittiklerine inanmaktadır.

Diğer çarpıcı bir örnek ise 2010 yılında İran'a yapılan Stuxnet saldırısıdır. Stuxnet olarak adlandırılan bir kurtçuk ile İran-Buşehr nükleer santralindeki sistemlerini etkilemek için özel amaçlar gözetilerek santralin ilgili sistemlerini farklı frekanslarda ve motor hızlarında çalıştıracak şekilde işlevsiz hale getirmek amacıyla, ABD Savunma Bakanlığı desteğiyle, bir grup gönüllü siber savaş yazılımcısı tarafından Alman-Siemens bilgi birikimi ve İsrail'in lojistiğiyle, USB bellekler-diskler ile yayılacak şekilde bu virüsün siber silah olarak hazırlandığı tahmin edilmektedir (Terzi, 2018, s.90-91).

Siber terörizmde altı çizilmesi gereken beş nokta bulunmaktadır. Bunlardan ilki, siber terörizmin yönelidiği hedeftir. Bu hedefler, ülkenin askeri gücü, hükümet, bireyler, şirketler, ülkenin önemli altyapı tesisleri gibi birçok şey olabilir. İkinci nokta ise, siber terörizmin hangi saiklerle hareket ettiğidir. Bu saikler ya da güdüler dini, politik, sosyal, kültürel ve ideolojik vb. olabilir (Şimşek, 2016, s.325).

Üçüncü nokta, siber terörizmde hangi vasıtaların kullanıldığıdır. Buna göre siber terörizmde kullanılan araçlar; bilgisayar, iletişim ağı ve teknolojisidir. Dördüncü önemli nokta ise, alt yapının yok edilmesi, askeri ve önemli bilgilerin ele geçilip sızdırılması, insanlara ya da şirketlere ait varlıların teröristlere ait hesaplara geçirilmesi gibi verilen zararla oluşturdukları etkidir. Son nokta ise, elde edilmek istenen amaçtır. Bu amaçlar her türlü politik, dini, askeri amaçlar olabilir (Şimşek, 2016, s.326).

Siber terörizm yöntemlerini kullanarak terör örgütlerinin bir barajın kapaklarını açarak tarım alanlarını kullanamaz hale getirecekleri, güvenlik güçlerinin haberleşme ağlarına sızarak yanıltıcı bilgiler yayabilecekleri, kentin bütün trafik ışıklarını durdurarak normal hayatı alt üst edebilecekleri, telefon şebekelerini kullanılmaz hale getirebilecekleri, elektrik ve doğalgaz hatlarını kapatabilecekleri ifade edilmektedir. Siber terörizm tanımlarından ve eylem alanlarından bu terörizm türünün gelecekte daha da etkin hale gelebileceği, terörizmin silahlı kanadına yönelik tedbirlerle birlikte siber alandaki faaliyetlerine yönelik de tedbirler geliştirmekte fayda görülmektedir.

Kaynakça

Atasever, S., Özçelik, İ., & Sağıroğlu, Ş. (2019). Siber Terör ve DDoS. Journal of Natural & Applied Sciences, 23(1).

Erendor, M. E. (2016). Risk toplumu ve refleksif modernleşme çerçevesinde siber terörizm: Tanımlama ve tipoloji sorunu. Cyberpolitik Journal, 1(1), 114-134.

Gürkaynak, M., & İren, A. A. (2011). *Reel dünyada sanal açmaz: Siber alanda uluslararası ilişkiler.* Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 16(2), 263-279.

Hatipoğlu, C. (2017). *Teknolojik savaşlar: Siber terörizm tehditleri*. In ICPESS (International Congress on Politic, Economic and Social Studies) (No. 3).

Özcan, M. (2002). *Siber terörizm ve ulusal güvenlik: İnternet ve hukuk*. İstanbul: Bilgi Üniversitesi Yayınları.

Şimşek, M. (2016). *Terörizm: Kavramsal Bir Çalışma*. Akademik Bakış Uluslararası Hakemli Sosyal Bilimler Dergisi, (54), 319-335.

Terzi, M. (2018). *Bilgi ve iletişim teknolojilerine dayalı oluşumlar ile bu oluşumların uluslararası ilişkilere güvenlik bağlamındaki etkisi: Siber terörizm.* Kara Harp Okulu Bilim Dergisi, 28(1), 73-108.

Yılmaz, B.A. (2020). *Siber terörizm ve değişen istihbarat anlayışı.* Anadolu Strateji Dergisi, 2(1), 65-82.

---

[i] Atıf için: TERAM. (2020). *Siber Terörizm Nedir?* Erişim adresi: https://www.teram.org/Icerik/siber-terorizm-nedir-91

TERAM